Grantham's problem(New development of research on Computer Algebra)

AUTHOR(S):

篠原, 直行

CITATION:

篠原, 直行. Grantham's problem(New development of research on Computer Algebra). 数理解析研究所講究録 2007, 1572: 1-10

ISSUE DATE:

2007-11

URL:

http://hdl.handle.net/2433/81312

数理解析研究所講究録
第1572巻 2007年 1-10

Grantham's problem

篠原 直行
NAOYUKI SHINOHARA*
CREST JST / 立教大学
CREST JST / RIKKYO UNIV.

Abstract

現在, 任意に与えられた自然数 n が素数であるか否かを効率よく判定するアルゴリズムがいくつか提案されているが, 計算量評価が $\mathcal{O}((\log n)^5)$ より小さく, かつ, 合成数を必ず「合成数である」と判定できるアルゴリズムは知られていない. したがって, 計算量評価が小さく判定結果も常に正しいアルゴリズムを構築することがこの分野において最終的な課題とされる.

本稿では, この課題の達成に重要な意味を持つ Grantham の問題に関するいくつかの結果を紹介する. 本稿は, この最終課題を達成する上で必要となるであろう, 既存のアルゴリズムの長所と短所, 著者の研究の方向付け, 現在までの成果に関する概説である.

1 序論

1.1 素数判定アルゴリズム

素数判定アルゴリズムとは, 任意に与えられた自然数が素数であるか否かを判定するアルゴリズムであり, その結果は確率的である. つまり, まれに合成数を合成数と判定できない場合が存在する. それは, この種のアルゴリズムが「n が素数であるならば, n に関する計算可能な条件が成り立つ」という定理の対偶を用いるからである.

例えば, Fermat test は下にあげる Fermat の小定理に基づいた素数判定アルゴリズムである.

定理 1.1. *n は素数とし, a は $\gcd(a,n)=1$ なる整数であるとする. このとき次の式が成り立つ.*

$$a^{n-1} \equiv 1 \pmod{n}. \tag{1}$$

従って, Fermat test は定理 1.1 の対偶を利用する, つまり与えられた自然数 n と $\gcd(a,n)=1$ なる適当に選んだ a に対して (1) が成り立つかを見るわけである. もし (1) が成り立たなければ n は合成数であることがただちにわかる. ただ, ここで注意しなければならないのは, (1) が n に対して成り立ったとしても n が必ずしも素数であるとは限らない点である.

例えば $2^{341-1} \equiv 1 \pmod{341}$ であるが $341 = 11 \cdot 31$ より素数ではない. このように合成数でありながら素数判定アルゴリズム T で合成数と判定されないものを T-擬素数と呼ぶ. さらに, Fermat test のように, 与えられたパラメータ P によって結果が異なる場合, それは P に対する T-擬素数と呼ばれる. (上の例の場合は, 341 は 2 に対する Fermat 擬素数であるという.)

素数判定アルゴリズムには, Strong Fermat test (Miller-Rabin test) [1], Quadratic Frobenius test [1] など, 計算量評価が $\mathcal{O}((\log n)^3)$ と小さいものが多いことがその特徴の一つにあげられる.

*shnhr@tvs.rikkyo.ne.jp

1.2 素数証明アルゴリズム

素数性を判定するもう一つの種のアルゴリズムに素数証明アルゴリズムがある. 先に述べた素数判定アルゴリズムとの違いは, 判定された結果が常に正しい, つまり素数証明アルゴリズムをパスしたものは必ず素数であるという点である. この意味で素数証明アルゴリズムは素数判定アルゴリズムより上位であるといえる. しかしながら, 計算量の点では素数判定アルゴリズムの方が素数証明アルゴリズムより優れているといえる. その理由を少し説明しよう.

Eratosthenes の篩（試し割）は非常にシンプルな素数証明アルゴリズムである. このアルゴリズムでは, 与えられた自然数 n が $\sqrt{n}$ 以下の全ての素数に対して割り切れるかどうかをみるため, $\mathcal{O}(\sqrt{n}/\log n)$ 回の割り算を必要とする. （この評価は素数定理より得られる.）従って, bit 演算の評価は $\mathcal{O}(\sqrt{n}\log n)$ となり, 実用的であるとは言えない. （素数性を判定するアルゴリズムの計算量は $\mathcal{O}((\log n)^5)$ 以下であることが望まれる.）

また, 同じく素数証明アルゴリズムである $n-1$ 法は, 判定対象を n としたときに $n-1$ が二つ以上の大きな素因子を持てば, n の素因数分解と同等の計算を必要とすることになるため, 当然ながらその計算量評価も素因数分解を考えた場合のものと等しくなり $\log n$ 多項式時間とはならない.

近年, 注目を浴びた AKS 法 [2] は, 任意に与えられた判定対象 n に対して計算量評価が $\log n$ 多項式時間であらわされる現在唯一の素数証明アルゴリズムである. しかし, このアルゴリズムも計算量評価が $\mathcal{O}((\log n)^5)$ 以下ではないため実用的なアルゴリズムとは言い難いものである.

他にも, 楕円曲線法 [3],[4], Jacobi sums test [5] など, 数値実験により計算量が $\mathcal{O}((\log n)^5)$ を下回ると予想されるものも存在するが, どれも未解決問題を抱え論理的に証明を与えられているものは知られていない.

1.3 素数判定アルゴリズムから素数証明アルゴリズムへの改良

素数判定アルゴリズムを改良することにより, 素数証明アルゴリズムを構築することは非常に興味深く有効な手法である. その一つに extended Riemann hypothesis と strong Fermat test を組み合わせたもの [6] がある. ただ, 残念なことに extended Riemann hypothesis は未解決であるため, この手法は素数証明アルゴリズムとしては認められていない.

定理 1.2. *extended Riemann hypothesis* が成り立つと仮定する. このとき n が奇合成数であるならば, *strong Fermat test* で n を合成数と判定できる $\gcd(a,n)=1$ なるパラメータ $a \in \mathbb{Z}$ が区間

$$[2, 2(\ln n)^2]$$

内に必ず存在する.

この定理 1.2 により, パラメータの変換は高々 $2(\ln n)^2$ 回であるため, 計算量評価は $\mathcal{O}(2(\log n)^2 \cdot (\log n)^3) = \mathcal{O}((\log n)^5)$ となる.

このようにパラメータの選び方に条件を付け加えることで, quadratic Frobenius test から素数証明アルゴリズムを構築することを試みるのは興味深いことである. Quadratic Frobenius test とは, J. Grantham によって提案された素数判定アルゴリズムで, 次の定理によるものである.

定理 1.3 a, b は $\Delta = a^2 - 4b \neq 0$ を満たす整数とする. また素数 n は $\gcd(n, 2b\Delta) = 1$ を満たすものとする. このとき次の合同式が成り立つ.

$$x^n \equiv \begin{cases} a - x \pmod{(x^2 - ax + b, n)}, & (\left(\frac{\Delta}{n}\right) = -1 \text{ のとき}), \\ x \pmod{(x^2 - ax + b, n)}, & (\left(\frac{\Delta}{n}\right) = 1 \text{ のとき}) \end{cases} \tag{2}$$

この定理からわかるように quadratic Frobenius test は Frobenius autmorphism の性質を用いたものである. さらに, 多項式剰余環 $(\mathbb{Z}/n\mathbb{Z})[x]/(x^2-ax+b)$ 上での計算を行うことからわかるように, 整数の組 (a,b) は Frobenius test におけるパラメータである.

最終的に我々が知りたいのは, 任意に与えられた合成数 n が $\mathcal{O}((\log n)^2)$ 回以下のパラメータ変換で必ず (2) が成り立たないようなパラメータ (a,b) を得る方法である. そのためには, まず合成数 n が Frobenius 擬素数となるときのパラメータ (a,b) と n の関係を知ることが重要である. [7] では, Frobenius 擬素数を五つの場合に分類し, それぞれに対する同値条件, つまり n,a,b の関係を明らかにした.

また, Grantham の問題 [1] は, 一組のパラメータ $(-5,5)$ で $n \equiv \pm 2 \pmod 5$ なる全ての自然数 n に対して quadratic Frobenius test は素数証明アルゴリズムになる可能性があることを示唆している.

本稿では 2 つの相異なる奇素数の積の場合について Grantham の問題を検証して得られた結果について紹介する.

2 Quadratic Frobenius 擬素数

この章では, Quadratic Frobenius test に関するいくつかの性質などを紹介する.

2.1 Quadratic Frobenius test

Quadratic Frobenius test は, J. Grantham [1] によって提案された, 定理 1.3 に基づく素数判定アルゴリズムである. ここで, n が $\gcd(n, 2b\Delta) = 1$ でありながら式 (2) を満たすものが存在し, それを (a,b) に対する quadratic Frobenius 擬素数と呼ぶ. 以後, 簡単のため単に (a,b) に対する Frobenius 擬素数とよび, $fpsp(a,b)$ とかく.

[1] の定義では $\Delta = a^2 - 4b$ は平方数でないとしているが, Δ が平方数であるときは, Frobenius test が Fermat test と常に同等となるだけである. また, Δ が平方数でなくても, 判定対象 n の任意の素因子 p を法として Δ が平方剰余であれば, Frobenius test は Fermat test と同等になる. 従って, 本稿の定義では Δ が平方数であるか否かを区別しないものを採用した. ただ, $\Delta \neq 0$ としているのは Frobenius test で $\gcd(n, 2b\Delta) = 1$ という条件を使うからである.

以後は考えやすくするため次の補題 2.1 の条件 (3) に注目する.

補題 2.1. *a,b は $\Delta = a^2 - 4b \neq 0$ を満たす整数とする. このとき $\gcd(n, 2b\Delta) = 1$ なる合成数 n が $fpsp(a,b)$ であることと以下の合同式が成り立つことは同値である.*

$$x^{n-(\frac{\Delta}{n})} \equiv \begin{cases} b \pmod{(x^2-ax+b, n)} & ((\frac{\Delta}{n}) = -1 \text{ のとき}), \\ 1 \pmod{(x^2-ax+b, n)} & ((\frac{\Delta}{n}) = 1 \text{ のとき}). \end{cases} \tag{3}$$

2.2 Frobenius 擬素数と円分多項式

先に述べたように, $fpsp(a,b)$ となる奇合成数とそのときの整数の組 (a,b) との関係を知りたいわけであるが, 素冪環における円分多項式の "因子" の性質を考えることによりその関係が明らかになる. (ただ, 素

冪環 $\mathbb{Z}/p^e\mathbb{Z}$ は $e>1$ のときは整域ではないため, 素冪環での多項式の "既約性" や "因子" の取り扱いには一般には注意が必要である. しかし, 本稿で取り扱う内容においては通常の規約性や因子と同様に考えても問題はない. 従って以後は単に因子と書く.)

Frobenius test による n の判定結果は $(\mathbb{Z}/n\mathbb{Z})[x]/(x^2-ax+b)$ における x の位数に左右される. 当然ながら x は有限位数をもちそれを M とし, 第 m 円分多項式を $\Phi_m(x)$ と書くこととすれば,

$$x^M-1=\prod_{m\mid M}\Phi_m(x)\equiv 0 \pmod{(x^2-ax+b,p^e)}$$

が n の任意の素冪因子 p^e に対して成り立つ. つまり, x^2-ax+b は $\mathbb{Z}/p^e\mathbb{Z}$ において x^M-1 の因子であり, さらに x^M-1 が円分多項式の積でかけることに注目したわけである.

結論から先に言うと, $\mathbb{Z}/p^e\mathbb{Z}$ における第 m 円分多項式 $\Phi_m(x)$ の因子は, Hensel の補題によって, $\mathbb{F}_p$ 上の因子からリフトアップしたものである.

Frobenius 擬素数と円分多項式の関係に関する詳しい内容は [7] を参照していただきたい. ここでは, 本稿で使われる定義や記号を紹介する.

何度も言うように, $e>1$ のとき $\mathbb{Z}/p^e\mathbb{Z}$ は整域ではない. しかし, モニックな多項式については既約性などが以下のように自然に定義できる.

定義 2.2. $g(x)$ と $h(x)$ はモニックな整数係数多項式であるとする. $h(x)\equiv 0 \pmod{(p^e,g(x))}$ であるとき, "$g(x)$ は $\mathbb{Z}/p^e\mathbb{Z}$ 上で $h(x)$ をわりきる" といい, $g(x)\mid_{p^e} h(x)$ とかく.

定義 2.3. $g(x)$ をモニックな整数係数多項式であるとする. このとき,

$$g(x)\equiv s(x)t(x) \pmod{p^e} \text{ and } 0<\deg s<\deg g.$$

なる整数係数多項式 $s(x),t(x)$ が存在しないとき, "$g(x)$ は $\mathbb{Z}/p^e\mathbb{Z}$ 上既約である" という.

$x\in(\mathbb{Z}/p^e\mathbb{Z})[x]/(f(x))$ の位数は, $f(x)$ もしくはその一次因子がどの円分多項式割り切るかを決める重要な役割を持つ.

定義 2.4 $\alpha\in(\mathbb{Z}/p^e\mathbb{Z})^*$ の位数を

$$ord(p^e,\alpha)$$

と書く.

言い換えれば, $\alpha^{ord(p^e,\alpha)}=1$ かつ $1<\forall k\le ord(p^e,\alpha)-1$ に対して $\alpha^k\neq 1$ である.

定義 2.5 $g(x)\in(\mathbb{Z}/p^e\mathbb{Z})[x]$ はモニックで $(\mathbb{Z}/p^e\mathbb{Z})$ 上で既約であるものとする. このとき, $\alpha\in((\mathbb{Z}/p^e\mathbb{Z})[x]/(g(x)))^*$ の位数を

$$ord(p^e,g(x),\alpha).$$

とかく.

言い換えると, $\alpha^{ord(p^e,g(x),\alpha)}=1$ かつ $1<\forall k\le ord(p^e,g(x),\alpha)-1$ に対して $\alpha^k\neq 1$ である.

2.3 Frobenius 擬素数と ICF

この節では Frobenius 擬素数の分類と, 与えられた (a,b) に対して奇合成数 n が各種の Frobenius 擬素数になるときの同値条件 $(ICF1)$ から $(ICF5)$ を紹介する.

$1 \leq a,b \leq 10$ かつ $\Delta = a^2-4b$ が平方数にならない組 (a,b) それぞれに対して, 区間 $[50000, 10^8+50000]$ 内のすべての奇合成数に対して Frobenius test を行った. その結果, $fpsp(a,b)$ の個数が 1000 を超える (a,b) の特徴がわかった. それは, $b=1$ となる場合の (a,b) か Lucas sequence が退化数列となる場合の (a,b) である. 後者の原因は Lucas test の性質によるものである. さらに, $b=-1$ となる場合の同様の実験結果では, $fpsp(a,-1)$ の個数は 500 個を超えることがわかった. これらの (a,b) に対する Frobenius 擬素数の個数は, 他の (a,b) に対して非常に大きなものである. またこれらの実験結果から, $(\frac{\Delta}{n}) = -1$ かつ $b \neq \pm 1$ なる $n = fpsp(a,b)$ は 291409 のみであることは興味深い事実である.

これらの結果から, $b = \pm 1$ と $(\frac{\Delta}{n})$ の値に注意して, Frobenius 擬素数を以下の五つに分類した. 各種の Frobenius 擬素数は互いに背反である.

定義 2.6 (Frobenius pseudoprime of the first type). n は $fpsp(a,b)$ で, さらに n の全ての素因子 p に対して $(\frac{\Delta}{p}) = 1$ が成り立つものとする. このとき, n を (a,b) に対する *Frobeius pseudoprime of the first type* とよび, さらに $fpsp1(a,b)$ とかく.

定義 2.7 (Frobenius pseudoprime of the second type). n は $fpsp(a,b)$ で, さらに n の少なくとも 1 つの素因子 p に対して $(\frac{\Delta}{p}) = -1$ が成り立つものとする. このとき, n を (a,b) に対する *Frobeius pseudoprime of the second type* とよび, さらに $fpsp2(a,b)$ とかく.

定義 2.8 (Frobenius pseudoprime of the third type). n は $fpsp(a,b)$ で, さらに $b \equiv 1 \pmod{n}$ と $(\frac{\Delta}{n}) = -1$ が成り立つものとする. このとき, n を (a,b) に対する *Frobeius pseudoprime of the third type* とよび, さらに $fpsp3(a,b)$ とかく.

定義 2.9 (Frobenius pseudoprime of the fourth type). n は $fpsp(a,b)$ で, さらに $b \equiv -1 \pmod{n}$ と $(\frac{\Delta}{n}) = -1$ が成り立つものとする. このとき, n を (a,b) に対する *Frobeius pseudoprime of the fourth type* とよび, さらに $fpsp4(a,b)$ とかく.

定義 2.10 (Frobenius pseudoprime of the fifth type). n は $fpsp(a,b)$ で, さらに $b \not\equiv \pm 1 \pmod{n}$ と $(\frac{\Delta}{n}) = -1$ が成り立つものとする. このとき, n を (a,b) に対する *Frobeius pseudoprime of the fifth type* とよび, さらに $fpsp5(a,b)$ とかく.

知りたいのは, 与えられた奇合成数 n が $fpsp(a,b)$ となる (n,a,b) の組の条件である. そのような条件を以下のように定義した.

定義 2.11 (Inefficasious conditions of Frobenius test (ICF)). いくつかの条件を満たす全ての数が *Frobenius* 擬素数となるものが存在し, それらの条件を "Inefficacious Conditions of Frobenius test (ICF)" とよぶ.

例えば, $(a,b) = (1,1)$ かつ合成数 n が $\gcd(n,6) = 1$ を満たすという条件は ICF である. なぜならば, その条件の下では n が $fpsp(1,1)$ だからである.

ここでは, 各タイプの Frobenius 擬素数の同値条件をぞれぞれ, $ICF1$ から $ICF5$ までで与える.

定義 2.12 (ICF of the first type $(ICF1)$**).** a,b は整数で $f(x)=x^2-ax+b$ とし, n は奇合成数でその素因数分解を $n=\prod_{i=1}^{k}p_i^{e_i}$ とあらわす. このとき (n,a,b) に関する以下の条件一組を *"ICF1"* とよぶ.
$(ICF1-1)$ 各 $i\in[1,k]$ に対して, $f(x)\equiv(x-c_{i,1})(x-c_{i,2}) \pmod{p_i^{e_i}}$ かつ $c_{i,1}\not\equiv c_{i,2} \pmod{p_i^{e_i}}$ で,

$$x-c_{i,1}\mid_{p_i^{e_i}}\Phi_{m_i}(x),\ x-c_{i,2}\mid_{p_i^{e_i}}\Phi_{m_i'}(x)$$

をみたす自然数 m_i,m_i' が存在する.
$(ICF1-2)$ $m=lcm(m_1,m_1',...,m_k,m_k')$ に対して $n\equiv 1 \pmod{m}$.

奇合成数 n が $fpsp1(a,b)$ であることと, (n,a,b) に対して $ICF1$ が成り立つことは同値である.

定義 2.13 (ICF of the second type $(ICF2)$**).** a,b は整数で $f(x)=x^2-ax+b$ とし, n は奇合成数でその素因数分解を $n=\prod_{i=1}^{k+\ell}p_i^{e_i}$ とあらわす. このとき (n,a,b) に関する以下の条件一組を *"ICF2"* とよぶ.
$(ICF2-1)$ 各 $i\in[1,k]$ に対して, $f(x)$ は $\mathbb{Z}/p_i^{e_i}\mathbb{Z}$ 上既約で, $f(x)\mid_{p_i^{e_i}}\Phi_{m_i}(x)$ なる m_j が存在する.
$(ICF2-2)$ $\sum_{i=1}^{k}e_i\equiv 0 \pmod 2$ が成り立つ.
$(ICF2-3)$ 各 $i\in[k+1,k+\ell]$ に対して, $f(x)\equiv(x-c_{i,1})(x-c_{i,2}) \pmod{p_i^{e_i}}$ かつ $c_{i,1}\not\equiv c_{i,2} \pmod{p_i^{e_i}}$ で,

$$x-c_{i,1}\mid_{p_i^{e_i}}\Phi_{m_i}(x),\ x-c_{i,2}\mid_{p_i^{e_i}}\Phi_{m_i'}(x)$$

なる自然数 m_i,m_i' が存在する.
$(ICF2-4)$ $m=lcm(m_1,...,m_k,m_{k+1},m_{k+1}',...,m_{k+\ell},m_{k+\ell}')$ に対して $n\equiv 1 \pmod{m}$ が成り立つ.

奇合成数 n が $fpsp2(a,b)$ であることと, (n,a,b) に対して $ICF2$ が成り立つことは同値である.

定義 2.14 (ICF of the third type $(ICF3)$**).** a,b は整数で $f(x)=x^2-ax+b$ とし, n は奇合成数でその素因数分解を $n=\prod_{i=1}^{k+\ell}p_i^{e_i}$ とあらわす. このとき (n,a,b) に関する以下の条件一組を *"ICF3"* とよぶ.
$(ICF3-1)$ 各 $i\in[1,k]$ に対して, $f(x)$ は $\mathbb{Z}/p_i^{e_i}\mathbb{Z}$ 上既約で, さらに $p_i\equiv -1 \pmod{m_i}$, $f(x)\mid_{p_i^{e_i}}\Phi_{m_i}(x)$ なる自然数 $m_i>2$ が存在する.
$(ICF3-2)$ $\sum_{i=1}^{k}e_i\equiv 1 \pmod 2$ が成り立つ.
$(ICF3-3)$ 各 $i\in[k+1,k+\ell]$ に対して, $f(x)\equiv(x-c_i)(x-c_i^{-1}) \pmod{p_i^{e_i}}$ で, さらに $x-c_i\mid_{p_i^{e_i}}\Phi_{m_i}(x)$ なる自然数 $m_i>2$ が存在する.
$(ICF3-4)$ $m=lcm(m_1,...,m_{k+\ell})$ に対して $n\equiv -1 \pmod{m}$ が成り立つ.

奇合成数 n が $fpsp3(a,b)$ であることと, (n,a,b) に対して $ICF3$ が成り立つことは同値である.

定義 2.15 (ICF of the fourth $(ICF4)$**).** a,b は整数で $f(x)=x^2-ax+b$ とし, n は奇合成数でその素因数分解を $n=\prod_{i=1}^{k+\ell}p_i^{e_i}$ とあらわす. このとき (n,a,b) に関する以下の条件一組を *"ICF4"* とよぶ.
$(ICF4-1)$ 各 $i\in[1,k]$ に対して, $f(x)$ は $\mathbb{Z}/p_i^{e_i}\mathbb{Z}$ 上既約で, $f(x)\mid_{p_i^{e_i}}\Phi_{m_i}(x)$ と

$$s_i\geq 2,\ p_i\equiv 2^{s_i-1}r_i-1 \pmod{m} \text{ かつ } m_i\neq 4$$

を満たす自然数 $m_i=2^{s_i}r_i$ が存在する. ただし r_i は奇数とする.
$(ICF4-2)$ $\sum_{i=1}^{k}e_i\equiv 1 \pmod 2$ が成り立つ.
$(ICF4-3)$ 各 $i\in[k+1,k+\ell]$ に対して, $f(x)\equiv(x-c_i)(x+c_i^{-1}) \pmod{p_i^{e_i}}$ で, さらに $x-c_i\mid_{p_i^{e_i}}\Phi_{m_i}(x)$ なる自然数 m_i が存在する.
$(ICF4-4)$ $m=lcm(m_1,...,m_{k+\ell})$ に対して, $n\not\equiv -1 \pmod{m}$, $2(n+1)\equiv 0 \pmod{m}$ が成り立つ.

奇合成数 n が $fpsp4(a,b)$ であることと, (n,a,b) に対して $ICF4$ が成り立つことは同値である.

定義 2.16 (ICF of the fifth type $(ICF5)$**).** a,b は整数で $f(x)=x^2-ax+b$ とし, n は奇合成数でその素因数分解を $n=\prod_{i=1}^{k+\ell}p_i^{e_i}$ とあらわす. このとき (n,a,b) に関する以下の条件一組を *"$ICF5$"* とよぶ.
$(ICF5-1)$ 各 $i\in[1,k]$ に対して, $m_i \mid \gcd(p_in-1,p_i^2-1)$, $m_i\nmid p_i-1$ なる自然数 m_i が存在する.
$(ICF5-2)$ 各 $i\in[1,k]$ に対して, $f(x)$ は $\mathbb{Z}/p_i^{e_i}\mathbb{Z}$ 上既約で, さらに $f(x)\mid_{p_i^{e_i}}\Phi_{m_i}(x)$ が成り立つ.
$(ICF5-3)$ $\sum_{i=1}^{k}e_i\equiv 1 \pmod 2$ が成り立つ.
$(ICF5-4)$ 各 $i\in[k+1,k+\ell]$ に対して, $m_i \mid \gcd(n^2-1,p_i-1)$, $m_i\nmid n-1$ をみたす自然数 m_i が存在する.
$(ICF5-5)$ 各 $i\in[k+1,k+\ell]$ に対して, $f(x)\equiv(x-c_i)(x-c_i^n) \pmod{p_i^{e_i}}$ となり, さらに $f(x)\mid_{p_i^{e_i}}\Phi_{m_i}(x)$ なる整数 m_i が存在する.
$(ICF5-6)$ $b\not\equiv\pm1 \pmod n$ が成り立つ.

奇合成数 n が $fpsp5(a,b)$ であることと, (n,a,b) に対して $ICF5$ が成り立つことは同値である.

3 Grantham の問題と $ICF5$

Frobenius test から素数証明アルゴリズムを構築する上で非常に興味深い以下のような問題がある.

問題 3.1 (Grantham の問題) $n\equiv\pm2 \pmod 5$ なる奇合成数 n で $fpsp5(-5,5)$ となるものは存在するか.

Dirichlet の算術級数定理より, $n_i\equiv\pm2 \pmod 5$ なる素数 n_i と $n_j\equiv\pm1 \pmod 5$ なる素数 n_j の存在比率は等しい. 従って, Grantham の問題の条件を満たすような合成数が存在しなければ, Frobenius test は半分の素数に対する計算量 $\mathcal{O}((\log n)^3)$ の素数証明アルゴリズムに改良できることになる.

3.1 $ICF5$ と $(\frac{b}{n})=-1$

n が $n\equiv\pm2 \pmod 5$ を満たすならば, $(\frac{5}{n})=-1$ が成り立つ. このとき, さらに n が $fpsp(-5,5)$ である場合について考えることから, $\Delta=b=5$ より, n が $fpsp5(a,b)$ でかつ $(\frac{b}{n})=-1$ なる場合について考える必要がある. この節では後で必要となる二つの結果を紹介する.

補題 3.2 n は $fpsp5(a,b)$ であるものとする. また p は n の素因子で $(\frac{\Delta}{p})=1$ を満たすものとする. このとき

$$\left(\frac{b}{p}\right)=1.$$

補題 3.3 $\Delta=a^2-4b\neq0$ で $f(x)=x^2-ax+b$ とする. また, 奇素数 q は $(\frac{\Delta}{q})=(\frac{\Delta}{q})=-1$ を満たすものとする. このとき, $x\in(\mathbb{Z}/q\mathbb{Z})[x]/(f(x))$ の乗法位数を m とし, 自然数 s と奇数 t で $q^2-1=2^st$ と書くとき, m は 2^s で割り切れる.

ここで, q^2-1 は必ず 8 で割り切れることから次の系を得る.

系 3.4 $\Delta=a^2-4b\neq0$ で $f(x)=x^2-ax+b$ とする. また, 奇素数 q は $(\frac{\Delta}{q})=(\frac{\Delta}{q})=-1$ を満たすものとする. このとき, $x\in(\mathbb{Z}/q\mathbb{Z})[x]/(f(x))$ の乗法位数 m は 8 で割り切れる.

3.2 $n = pq$ 型の Grantham の問題

Grantham の問題を, 最もシンプルと思われる, 二つの相異なる奇素数 p, q の積 n について考えてみる. Grantham の問題では $fpsp5(-5, 5)$ なるものを考えている.

事実 3.5 n が $fpsp(a, b)$ ならば n は $fpsp(-a, b)$ である.

著者が持っている数値実験のデータの都合により, Grantham の問題を $fpsp5(5, 5)$ の場合に置き換えて議論を進めていく.

$f(x) = x^2 - 5x + 5$ とし, $n = pq$ は $fpsp5(5, 5)$ で奇素数 p, q はそれぞれ $(\frac{5}{p}) = 1$, $(\frac{5}{q}) = -1$ を満たすものとする. 従って,

$$p \equiv \pm 1 \pmod 5, \tag{4}$$

$$q \equiv \pm 2 \pmod 5 \tag{5}$$

が成り立っている. また $\Delta = 5$ であることから, $f(x)$ は p を法として可約であり, q を法としたときは既約である. 従って, ある整数 c_1, c_2 が存在して $f(x) \equiv (x - c_1)(x - c_2) \pmod p$ と書ける.

さて, ここから n, a, b に対して $ICF5$ の条件を検証していく.

まず $(ICF5-3)$ と $(ICF5-6)$ は明らかに成り立つ.

次に $(ICF5-2)$ については, 先ほど述べたように $f(x)$ が $\mathbb{F}_q$ 上既約であることは問題ない. さらに, 実は $m_q = ord(q, f(x), x)$ とすれば $f(x)$ は q を法として第 m_q 円分多項式 $\Phi_{m_q}(x)$ を割り切る. 従って $(ICF5-1)$ において, この m_q が条件を満たしているかどうかが論点となる. $\Phi_{m_q}(x)$ が $\mathbb{F}_q$ 上で相異なる二次の規約因子に因数分解されることと $m_q \mid q^2 - 1$, $m_q \nmid q - 1$ は同値であることから, $m_q \mid qn - 1$, つまり

$$m_q \mid p - 1 \tag{6}$$

が成り立たなければならない.

残るは $(ICF5-4)$ と $(ICF5-5)$ の確認である. $(ICF5-5)$ より $c_1^n \equiv c_2 \pmod p$ で, $m_p = ord(p, c_1)$ とすると $f(x)$ は p を法として第 m_p 円分多項式 $\Phi_{m_p}(x)$ を割り切る. これらの条件は, 実は

$$c_1^q \equiv c_2 \pmod p,\ c_2^q \equiv c_1 \pmod p \tag{7}$$

と同値である. $(ICF5-4)$ から, $m_p \mid \gcd(n^2 - 1, p - 1) = \gcd(q^2 - 1, p - 1)$, $m_p \nmid q - 1$ が成り立たなければならないことになるが, この場合は必ず成り立つので問題ない. 理由は次に述べるとおりである. $(x - c_1)(x - c_2)$ が p を法として $\Phi_{m_p}(x)$ を割り切るということは, $\Phi_{m_p}(x)$ が p を法として相異なる一次多項式の積に因数分解されることを意味する. $((\frac{\Delta}{p}) \neq 0$ であることから $c_1 \not\equiv c_2 \pmod p$ であることに注意. $)$ 従って, この場合, m_p は $p - 1$ を割り切ることとなる. $m_p \nmid q - 1$ については, 逆に $m_p \mid q - 1$ と仮定すると $c_2 \equiv c_1^q \equiv c_1 \pmod p$ となり矛盾が生じる. そして $m_p \mid q^2 - 1$ については (7) が成り立てば明らかに成り立つ.

最後に, $(\frac{b}{n}) = (\frac{5}{n}) = 1$ であることから, 系 3.4 より m_q は 8 で割り切れなければならい. さらに $m_q \mid p - 1$ と $p \equiv \pm 1 \pmod 5$ の条件から

$$p \equiv 1, 9 \pmod{40} \tag{8}$$

を得る.

以上より次の定理を得る.

定理 3.6 $n = pq$ は $fpsp5(5,5)$ であるとし, $(\frac{5}{p}) = 1$ と $(\frac{5}{q}) = -1$ が成り立つものとする. さらに, $f(x) = x^2 - 5x + 5 \equiv (x - c_1)(x - c_2) \pmod{p}$ とし, $m_q = ord(q, f(x), x)$, $m_p = ord(p, c_1)$ とおく. このとき以下の条件が成り立つ.

$$
\begin{aligned}
&(I) && p \equiv 1,9 \pmod{40},\ q \equiv 2,3 \pmod{5},\\
&(II) && m_q \mid p-1,\\
&(III) && c_1^q \equiv c_2 \pmod{p}\ and\ c_2^q \equiv c_1 \pmod{p}.
\end{aligned}
$$

この定理の条件を満たす素数の組 (p,q) が存在すれば, pq が Grantham 問題の条件を満たす Frobenius 擬素数となるわけである.

では, そのようなそのような素数の組を探すことを考えよう.

定理 3.6 の $(I), (III)$ より, p に関する条件が q に関する条件より厳しいと考えられる. 従って, 最初に p の候補となりうる素数を探すのが望ましい. つまり, $p \equiv 1,9 \pmod{40}$ なる素数 p を探し, p を法として $f(x) = x^2 - 5x + 5$ を因数分解する. このとき, $p \equiv \pm 1 \pmod{5}$ であることから, $f(x)$ は必ず $(x - c_1)(x - c_2)$ のように因数分解され, これは m_p が $p-1$ を割り切ること意味する. ここで c_1, c_2 が (III) を満たすかどうかをチェックしなければならないのだが, この時点では q が未定であるため, 代わりに

$$c_1^t \equiv c_2 \pmod{p},\ c_2^t \equiv c_1 \pmod{p} \tag{9}$$

を満たすような t が存在するか否かをチェックする. 存在しなければ, 最初のステップへもどり p を選びなおすことから始める.

ここまでで, p に関するチェックはすべて終了である. 次は, p に対して (I) から (III) を満たす素数 q を探すことになる. (III) と (9) より

$$q \equiv t \pmod{m_p},$$

が成り立たなければならない. また (I) より $q \equiv \pm 2 \pmod{5}$ も満たさなければならない. もしここまでの条件を満たす q が存在しなければ最初のステップへ, 存在するならば m_q を求めて $m_q \nmid p-1$ の確認を行う. もちろん満たされなければ最初のステップへ戻り, 成り立てば p, q を返し, $n = pq$ が $fpsp5(5,5)$ となる.

以上よりアルゴリズムは以下のようになる.

アルゴリズム 3.7

1, $p \equiv 1 \pmod{40}$ なる素数 p を求める.
2, $x^2 - 5x + 5$ を p を法として因数分解し $(x - c_1)(x - c_2)$ をえる.
3,

$$c_1^t \equiv c_2 \pmod{p},\ c_2^t \equiv c_1 \pmod{p}$$

を満たす整数 t を求める. 存在しなければ 1 へ.
4, $c_1 \in \mathbb{F}_p$ の乗法位数 m_p を計算する.
5,

$$q \equiv t \pmod{m_p},\ q \equiv \pm 2 \pmod{5} \tag{10}$$

を満たす素数 q を求める. 存在しなければ 1 へ.
6, $x \in \mathbb{F}_q[x]/(f(x))$ の乗法位数 m_q を計算する.
7, $m_q \mid p-1$ を満たせば pq を返し, 満たさなければ 1 へ.

(8) を満たす $[0,10^9]$ 内の全ての素数 p に対して数値実験を行ったところ, 候補となりうるのは 521, 221401 の二つのみであった. つまり, これらの素数を p とすると,

$$p \equiv 1,9 \pmod{40},$$
$$\exists t \in \mathbb{Z}, c_1^t \equiv c_2 \pmod{p}, c_2^t \equiv c_1 \pmod{p}.$$

が成り立つ. 従って, あとは p と組をなす q は何かということになるが, 実は 521 や 221401 と組をなす素数 q が存在しないことがわかる.

各 (p,t,m_p) は $(521,181,260)$ と $(221401,17549,36900)$ である. ここで, どちらの場合も $t \equiv \pm 1 \pmod 5$ かつ $5 \mid m_p$ であることに気付く. これは (10) を満たす q が存在しないことを意味する.

従って次の定理を得る.

定理 3.8 $n = pq$ で, p と q はそれぞれ $(\frac{5}{p}) = 1$, $(\frac{5}{q}) = -1$ を満たすものとする. このとき, もし n が $fpsp5(5,5)$ であるならば $p > 10^9$ である. ∎

4 まとめ

本稿では $n = pq$ 型の場合の $fpsp5(5,5)$ についてふれたが, 実験により p となりうる候補の存在を確認することができなかった. 仮に存在したとしてもそれは極めてまれであると推測される. 今後の研究課題は, より広範囲で p の候補を探すこととなるが, q に関して絞り込みができる条件について考えることも重要である.

q に関する条件の考察は $n = q_1q_2q_3$ で $(\frac{\Delta}{q_i}) = -1$ $(i = 1,2,3)$ について考える上で重要となる. 当然のことながら, $n = pq$ 型以外の場合でも $ICF5$ によって, $fpsp5(5,5)$ の素因子が持つ条件がわかり, それをもとに素因子の候補を計算することができる.

参 考 文 献

[1] R. Crandall and C. Pomerance. *Lucas pseudoprimes*, Pime Numbers (2001), 130-140.

[2] M. Agrawal, N. Kayal and N. Saxena. *PRIMES is in P*, (2002).

[3] A. O. L. Atkin and F. Morain. *Elliptic curves and primality proving*, (1993).

[4] F. Morain, *INRIA Research Report* 911, (1988).

[5] L. Adleman, C. Pomerance, and R. Rumely. *On distinguishing prime numbers from composite numbers.* Ann. of Math., 117 (1983), 173-206.

[6] E. Bach. Analytic Methods in the Analysis and Design of Number Theoretic Algorithms. A 1984 ACM Distinguished Dissertation. The MIT Press, (1985).

[7] N. Shinohara. *Frobenius pseudoprimes and cyclotomic polynomials.*, Math. Comp. (投稿中)

[8] J. Grantham. *A probable prime test with high confidence*, J. Number Theory, 72 (1998), 32-47.